APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: METHOD AND APPARATUS FOR ATTACHING ELECTRONIC SIGNATURE TO DOCUMENT HAVING STRUCTURE

APPLICANTS: TOMORU TERUUCHI AND KAZUNARI OIKAWA

METHOD AND APPARATUS FOR ATTACHING ELECTRONIC SIGNATURE TO DOCUMENT HAVING STRUCTURE

BACKGROUND OF THE INVENTION

The present invention relates generally to electronic signature (digital signature) technology utilized to ensure authenticity of an electronic file, and more particularly, to electronic signature technology applied to an electronic file which contains a document having a structure.

Electronic signature technology utilizes public key cryptosystem to certify that the contents of an electronic file have not been modified after an electronic signature was attached to the file. More specifically, for example, an electronic file or its digest is encrypted by a sender's private key, and its encrypted value is sent together with the original electronic file to a recipient, who decrypts the encrypted value by the sender's public key to see that the decrypted value is equal to the original electronic file or its digest, whereby it is certified that the contents of the original electronic file have not been modified.

Although the aforementioned conventional electronic signature technology can verify content equivalence between an electronic file and its encrypted electronic file, it cannot be used to verify document structure equivalence between files when the files contain a document having a structure.

Therefore, where there is document structure equivalence between electronic files although the electronic files are not equivalent to each other in terms of contents, the conventional technology can only verify that the contents of the electronic files do not match.

Further, as the conventional technology can describe only two kinds of states, i.e., equivalent or not equivalent, there is no way of knowing exactly which part of a document structure is different between files and how different they are, etc. when it transpires that the files are not equivalent.

SUMMARY OF THE INVENTION

In view of the situation as mentioned above, it is an object of the present invention to provide electronic signature technology to be applied to an electronic file containing a document having a structure, according to which a level of equivalence such as electronic file equivalence, document structure equivalence, document structure partial equivalence, etc. can be evaluated.

To achieve the above object, the present invention provides a method and apparatus for attaching an electronic signature to an electronic file containing a document having a structure, wherein a signature is generated from each structural element of a target document.

According to the electronic signature method of the present invention, first, a target document having a structure is analyzed to generate a representation using structural elements and then, a signature (encrypted structural element) is generated from each of structural elements of the generated representation and the thus generated signatures (ciphers) are concatenated to form a single signature corresponding to the structure of the document. A method of encrypting each structural element does not have to be limited to any particular method, and any common cipher generation method may be employed.

Further, according to the electronic signature method of the present invention, an electronic file with a generated electronic signature is verified and depending on a processing request, at least (1) electronic file equivalence, (2) document structure equivalence and (3) a coincidence rate between electronic files are found from the contents of the signature.

The electronic signature apparatus according to the present invention comprises electronic signature generator 11 and electronic signature analyzer 12, as illustrated in Fig. 1. The electronic signature generator 11 comprises parser unit 14 for analyzing target document having a structure 13 to generate a representation using structural elements; cipher generator unit 15 for generating a signature from each of structural elements generated by the

parser unit 14; and signature generator unit 16 for concatenating the generated signatures (ciphers) into a single signature corresponding to the structure of the document.

The electronic signature analyzer 12 similarly comprises parser unit 18 and signature analyzer unit 19 in order to verify electronic file 17 having a generated electronic signature. The signature analyzer unit 19 has at least three functions to perform in response to a request for processing, i.e. (1) function 21 of verifying electronic file equivalence ; (2) function 22 of verifying document structure equivalence ; and (3) function 23 of deriving a coincidence rate.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a conceptual diagram illustrating an electronic signature apparatus and the flow of process performed thereby;

Fig. 2 is a diagram illustrating a tree structure of a document;

Fig. 3 is a diagram showing an example of a structure of an XML file;

Fig. 4 is a diagram showing an example of a structure of a file which is equivalent to the structure of file shown in Fig. 3 in terms of XML although they are different files;

Fig. 5 is a diagram showing a document and a cipher corresponding to each structural element of the document;

Fig. 6 is a diagram showing an example of a format for concatenating electronic signatures (ciphers);

Fig. 7 is a diagram showing an XML file to which an electronic signature is attached;

Fig. 8 is a block diagram illustrating an example of a configuration of a system in which the present invention is reduced to practice;

Fig. 9 is a block diagram illustrating an example of a system configuration of an application example of the present invention;

Fig. 10 is a diagram showing an example of a

configuration.xml file to which an electronic signature is added;

Fig. 11 is a diagram showing an example of modification to a configuration.xml file; and

Fig. 12 is a diagram showing another example of modification to a configuration.xml file.

DETAILED DESCRIPTION OF THE INVENTION

First, reference is made to a "document having a structure", which constitutes a subject of a method and apparatus of the present invention. A normal document consists of chapters, sections and paragraphs, which may be diagrammatically represented as a tree structure as illustrated in Fig. 2. The electronic signature method and apparatus according to the present invention are directed to an electronic file containing a document that can be represented in the form of such a tree structure.

A file described in XML may be cited as an example of a document having such a tree structure. An example of an XML file is shown in Fig. 3.

In the shown example, the XML file contains information called "white space", that is, information about tab, line feed, etc. to represent indentation. Since XML permits the use of a white space in so far as the white space does not change a document structure, deletion of such information from this XML file does not affect its document structure per se. Fig. 4 shows the XML file with the white spaces being deleted, which is the same as the XML file shown in Fig. 3 in terms of a document structure. However, when these files in Figs. 3 and 4 are compared to each other simply as files, they are considered to be different.

Conventionally, whether or not two XML files are equivalent in terms of a document structure has been judged by analyzing them by means of an XML Parser, generating the result of the analysis in the form of DOM objects and comparing the thus generated DOM objects to see if they are equivalent. On the other hand, according to the electronic signature method and apparatus of the present invention,

the files in Figs. 3 and 4 have different signature codes representing a file although they have the same signature codes representing a document structure. Thus, by employing the present method and apparatus, it is possible to learn from the signature codes that these files are different in file contents and yet equivalent in terms of a document structure.

Fig. 5 shows an example of a signature of the aforementioned file and document structure. It is assumed here that Fig. 5 shows a result obtained by enciphering each structure element to be mapped to seventeen-digit decimal numerals. Next, a signature is generated based on the enciphered information. Fig. 6 shows a format for concatenating signatures (ciphers) to one another. In Fig. 6, a file signature code is a cipher indicative of coincidence in terms of a file, and "0xFF" is a delimiter for limiting a string of elements. Further, a depth code is a numerical value indicative of how much of a tree structure is ciphered to be contained in a signature. More specifically, when a depth code is 0, it signifies that ciphers to represent all the structural elements of a tree structure are included in a signature. By enabling this code to be set, precision of reliability judgment of a document with an electronic signature can be varied depending on the level of depth. A node signature code is a cipher of each element. By adding the thus constructed signature to the file as a structure element of the document, a document with an electronic signature shown in Fig. 7 is obtained. In the example shown in Fig. 7, a signature node, i.e.<Signature> ... </Signature> is added, and a symbol "+" is used to concatenate character strings for the sake of clarity of a construction of a signature, and the thus concatenated character strings constitute a signature.

The electronic signature apparatus according to the present invention may be built on a computer system 86 which comprises a CPU 81, a storage device 82, a file system 83, a display device 84 and an input device 85, as

illustrated in Fig. 8. In the file system 83, documents having electric signature as their data are stored/managed. Since the location of each document is not relevant to the substance of the present example, data may be placed in a database.

In the system configuration as illustrated above, the electronic signature method and apparatus according to the present invention can treat a file stored in the file system 83 as a document having a structure and verify whether an unauthorized modification has been made to the file and which portion of the structure has been modified if it transpires that there has been an unauthorized modification.

As a specific example of the aforementioned verification, reference is now made to an application example where an unauthorized operation of a system is prevented by verifying which portion of a file has been modified.

According to the application example, a tool for automatically generating a configuration for accessing a database system generates a configuration file containing an electronic signature, whereby a user is notified of an unauthorized modification on the file and the location of the unauthorized modification before access to the database system.

Conventionally, a configuration file, which is automatically generated by a tool for automatically generating a configuration for accessing a database system, does not support a modification made to a file by means of a method other than the tool. Usually, information indicative of whether or not a modification has been made to a file by a method other than the tool is not attached to a file. Besides, even if a conventional electronic signature is attached to such a configuration file, it can only show that a file has been modified and which portion of the file has been modified cannot be identified. Still further, as a conventional electronic signature can only verify that a file has been modified, even if the

modification does not disadvantageously affect an operation in the light of structural information, it is still indicated by the signature that the modification has been unauthorized. Thus, processing performed by a conventional electronic signature is not adequate or thorough.

Fig. 9 illustrates a system configuration of the above-described application example. Since the system illustrated in Fig. 9 comprises the system shown in Fig. 8 and database system 91, like numerals denote like components in Figs. 8 and 9. In order for the computer system 86 to access the database system 91, an appropriate configuration must be provided. The system in Fig. 9 is provided with a tool (ConfigGenTool) 92 for automatically generating such a configuration by interacting with a user. The tool 92 requests a user to enter information necessary for accessing the database system and generates a configuration file on the basis of the thus input information. More specifically, the tool 92 verifies that the computer system can access the database system 91 by the configuration and generates a configuration file (Config.xml) 93. At the time of generation of the configuration file 93, a user can indicate whether or not to add an electronic signature of the present invention to the configuration file 93 and also choose a depth code of the electronic signature which affects how extensively and strictly a structure of the file is to be covered by the electronic signature. Fig. 10 shows an example of the configuration file 93 to which an electronic signature is attached. In the example shown in Fig. 10, a signature of each structural element of a file and a signature of the file per se are both represented in seventeen-digit hexadecimal numbers.

The thus generated configuration file 93 is referenced by a database system access module (DBAccessor) 94, which is activated when the computer system actually accesses the database system 91. In this event, when an electronic signature is included in the configuration file 93, the module 94 verifies its authenticity before it

accesses the database system 91. When the configuration file 93 has been modified as shown in Fig. 11, the module 94 performs normal database access processing because the file of Fig. 11 coincides with the original file of Fig. 10 in terms of a structure, though the file of Fig. 11 is considered to be unauthorized in terms of a file coincidence, i.e. the files in Figs. 10 and 11 do not match. In other words, since the modification of the file in Fig. 10 to the file in Fig. 11 constitutes mere deletion of tabs and line feed codes, which are white spaces according to the XML specification, the files in Figs. 10 and 11 are equivalent in terms of XML.

On the other hand, when the configuration file 93 has been modified as indicated by the underline in Fig. 12, the module 94 can identify the modified portion in the file in Fig. 12 which does not coincide with the corresponding portion in the original file in Fig. 10 and notify a user by displaying a message "The designated provider is not authorized", before starting access processing. Thus, by using an electronic signature of the present invention in a configuration file for accessing a database system, a portion that has become unauthorized as a result of modification can be specifically indicated, whereby an unauthorized access can be avoided.

Further, the use of the electronic signature method and apparatus of the present invention enables determination as to whether each of structural elements of an electronic file containing a document having the above-described structure coincides with that of the original electronic file, whereby a coincidence rate or non-coincidence rate with respect to an entire structure as opposed to each structural element can be calculated and the system can be controlled with reference to the thus calculated rate.

As appreciated from the foregoing, according to the present electronic signature method and apparatus, electronic signatures can be extracted and compared, so that it becomes possible to verify equivalence between

electronic files containing a document having a structure such as file equivalence and document structure equivalence and also find a coincidence rate between files.